Network-1

حل وظيفة

تقديم:

مؤنس شحاذه مزهر

6160

Wireshark

- **ما هو؟**

محلل للبروتوكول الخاص بالشبكة بحيث يقوم بالتقاط حزمة معينة (شبكة) وعرض معلومات تفصيلية عنها وتعتبر أداة قوية بحيث تمكن من اكتشاف المشكلات الموجودة بالشبكة وإصلاحها.

- **حل الوظيفة:**

ملاحظة: سوف أقوم بالإجابة على الأسئلة الخاصة بالوظيفة على الملفات الذي اختبرناه في جلسات العملي وهو ملف (lab 3) ولذلك لفشل محاولاتي في تحميل نسخة pncp (من الموقع الرسمي و من الملف الذي حصلت عليه من الفلاشة)

1. ما هو عنوان IP المصدر و الوجهة لأول رسالة GET .

Source: 192.168.1.101
Dest: 128.119.245.12

2. ما هو عنوان IP المصدر و الوجهة الخاص برسالة الاستجابة الأولى.

Source: 2.23.13.5
Dest: 192.168.1.101

3. باستخدام الطوابع الزمنية لرسالة GET ورسالة الاستجابة المقابلة لها ، حدد المدة المستغرقة من وقت إرسال رسالة GET حتى تلقي رسالة الرد(قيمة عمود الوقت هو مقدار الوقت بالثواني منذ بدء تتبع Wireshark بشكل افتراضي).

Request Time = 7.981506s
Response Time = 7.981719s
=> x = ResT – ReqT = 0.000213s

4. حدد إصدار HTTP من إحدى الرسائل ، حدد عنوان URL لموقع الويب و وكيل المستخدم من أول رسالة GET .

HTTP/1.1

labs/HTTP-wireshark-file3.html

Mozilla/5.0

5. ما هو رقم تسلسل مقطع TCP SYN المستخدم في البدء اتصال TCP بين مضيفك والخادم؟ أي مجال في المقطع يعرّفها على أنها جزء SYN .

اعتقد انه لا يمكنني الإجابة على هذا السؤال لأن التقاط الحزمة لم يتم على جاهزي لقد استخدمت الفلتر التالي tcp.flags.syn == 1 and ip.src == <my ip address> ولم يظهر شيء

6. كم عدد مقاطع TCP المحتوية على البيانات اللازمة لنقل بيانات HTTP .

من الواضح أن الاجابة على هذا السؤال سوف تتطلب مني تحليل الحزمة على حاسوبي حيث لا يمكنني تحديد رقم محدد بدون تحليل الحزمة ولكنني لاحظت في احد الرسائل انه عن طريق قراءة ال info الخاص بها ثم الدخول على Transmission Control Protocol سوف يظهر احد المعلومات والتي هي [TCP segment length] وهو المعبر عن طول مقطع ال tcp

7. قم بملء المعلومات حول رسالة SYN–ACK :

Source IP address		20.67.219.150
Destination IP address		192.168.1.101
Source port number		443
Destination port number		49869
Sequence number		0
Acknowledgment number		1
Header length		32 bytes (8)
Window size		65535

8. اكتب udp في شريط الفلتر، ما هو المجموع الاختباري في عنوان UDP المستخدم وهل يمكن استخدامه لتسليم بيانات موثوق؟ ما هو حقل الطابع الزمني في رأس UDP المستخدم؟

4

لا يمكن الاعتماد عليه للمعلومات الموثوقة بالرغم من انه اسرع من tcp وذلك بسبب انه لا ينشأ اتصال بين المرسل والمستقبل قبل ارسال البيانات مما يفيد في المكالمات الصوتية والفيديو ولكنه لا يعتبر أمن للبيانات الحساسة لنفس السبب الذي يؤدي لسرعته

[timestamps]:

time since first frame = time since previous frame = 0

THE END.